UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
	:	
v.	:	
	:	**Mag. No. 13-8172**
LAURI LOVE,	:	
a/k/a "NSH,"	:	
a/k/a "ROUTE,"	:	
a/k/a "PEACE"	:	

I, David I. Oxley, being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that I am a Special Agent with the United States Army, Criminal Investigation Command, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

David I. Oxley, Special Agent
United States Army, Criminal Investigation Command

Sworn to before me and subscribed in my presence,
May 16, 2013, at Newark, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

From on or about October 1, 2012 through in or about February 2013, in the District of New Jersey and elsewhere, defendant

LAURI LOVE,
a/k/a "NSH,"
a/k/a "ROUTE,"
a/k/a "PEACE"

knowingly and intentionally conspired with others to commit an offense against the United States, that is,

a. to access a computer without authorization and to exceed authorized access, and thereby obtain information from a department or agency of the United States, namely, the United States Army, the value of which exceeds $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(iii);

b. to access a computer without authorization and to exceed authorized access, and thereby obtain information from a protected computer, namely, servers owned and operated by the United States Army, the value of which exceeds $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(iii).

Overt Acts

In furtherance of the conspiracy, and to effect its illegal objects, defendant and others (collectively "Co-Conspirators") committed the following overt acts in the District of New Jersey and elsewhere:

a. Beginning on or about December 23, 2012 and continuing through on or about December 26, 2012, the Co-Conspirators hacked into a computer server owned and operated by a component of the United States military. The Co-Conspirators used a computer server located in Parsippany, New Jersey to temporarily store malicious software that they then used to carry out the intrusion.

b. Beginning on or about October 6, 2012 and continuing through on or about October 7, 2012, the Co-Conspirators hacked into a computer server owned and operated by a component of the United States military. The data that the Co-Conspirators unlawfully accessed included personally identifiable information of military personnel stationed at Fort Monmouth, a military installation in Monmouth County, New Jersey.

In violation on of Title 18, United States Code, Section 371.

ATTACHMENT B

I, David I. Oxley, am a Special Agent with the United States Army Criminal Investigation Command ("Army CID"). The information contained in this Complaint is based upon my personal knowledge, as well as information obtained from other sources, including: a) statements made or reported by various witnesses with knowledge of relevant facts; b) my review of publicly available information; and c) my review of records and other documents obtained through subpoenas and other sources. Because this Complaint is being submitted for the limited purpose of establishing probable cause, it does not include every fact that I have learned during the course of the investigation. Where the content of documents and the actions, statements, and conversations of individuals are recounted herein, they are recounted in substance and in part, except where otherwise specifically indicated.

I. INTRODUCTION

1. From at least as early as approximately October 1, 2012 through in or about February 2013, LAURI LOVE, a/k/a "nsh," a/k/a "route," a/k/a "peace," and other individuals (collectively the "Co-Conspirators"), carried out a series of cyber attacks against the websites and computer systems of the United States Army. These cyber attacks involved, among other things, hacking into the Army's computer servers and stealing several massive quantities of confidential government data, including personally identifiable information of servicemen and servicewomen.

2. The Co-Conspirators also hacked into and stole data from computer servers of other United States agencies, both military and non-military, including the United States Sentencing Commission and the Federal Reserve.

II. BACKGROUND

3. Definitions:

a. An Internet Protocol ("IP") address is a unique numeric address used by a computer on the internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods. Every computer connected to the internet is assigned an IP address. The Internet also allows a person to specify a computer by a *name* rather than an IP address. This is known as the computer's "host name."

b. "Structured Query Language" ("SQL") is a programming language designed to retrieve and manage data on computer databases.

c. "SQL Injection Attacks" are methods of hacking into and gaining unauthorized access to computers connected to the Internet.

d. "HTML" is a computer programming language used to design websites.

e. "Malware" is malicious computer software programmed to, among other things, identify, store, and export information on computers that were hacked as well as to evade detection by anti-virus programs running on those computers.

f. "ColdFusion" is the name of a commercial web application development platform created by Adobe and designed to make it easier to connect simple HTML pages to a back-end database.

g. An Internet Relay Chat ("IRC") is an online medium through which multiple people can gather together in a "chat room" or "channel" and discuss topics of mutual interest. Similar to a telephone conference call, it allows multiple people to participate in and communicate within one "conversation," but words are typed not spoken.

4. At all times relevant to this Complaint:

a. The Engineer Research and Development Center ("Engineer R&D Center") was a research facility owned and operated by the U.S. Army Corps of Engineers ("Army Corps") in Vicksburg, Missouri.

b. The Plans and Analysis Integration Office ("PAIO") was a component of the United States Military ("USM") responsible for gathering and analyzing data, tracking the implementation of policies and overseeing long-range plans. The PAIO maintained a Research, Development and Engineering Command located in or around Aberdeen Proving Ground, Maryland.

c. The Strategic Studies Institute ("SSI") was a branch of the U.S. Army War College that published national security and strategic research and analysis. The SSI was located in Carlisle, Pennsylvania.

d. The Army Network Enterprise Technology Command ("NETCOM") planned, installed, integrated, protected and operated computer networks of the U.S. Army, and maintained a Network Enterprise Center located in or around Aberdeen Proving Ground, Maryland.

e. The Army Contracting Command ("ACC") provided contracting support to the U.S. Army throughout the United States and abroad. The ACC maintained the Army Materiel Command in or around Redstone Arsenal, Alabama.

III. THE MILITARY HACKS

5. As noted above, the Co-Conspirators hacked into computers belonging to several components of the USM during the period covered by this complaint. The investigation has revealed that the Co-Conspirators discussed, planned, and coordinated the military hacks using IRC.

A. The October 2, 2012 Engineer R&D Center Coldfusion Attack

6. Beginning on or about October 2, 2012 and continuing through on or about October 6, 2012, the Co-Conspirators attacked one of the Engineer R&D Center's servers, and compromised that server, by exploiting a known vulnerability in its ColdFusion application and unlawfully accessing an Army database.

7. After accessing these forbidden areas of the Engineer R&D Center's website, the Co-Conspirators obtained a copy of the password properties file. This file enabled the Co-Conspirators to determine the administrator password for the Engineer R&D Center's website. Using the stolen administrator's password, the Co-Conspirators obtained data belonging to the Army Corps, including information regarding the planned demolition and disposal of certain military facilities.

B. Law Enforcement Connects LAURI LOVE to the R&D Center Coldfusion Attack

8. The above-referenced attack on the Engineer R&D Center server originated from an IP address in Romania (the "Romanian IP Address"). The investigation has revealed that the Romanian IP Address was associated with the domain name "*ch0wn.dyndns.org*" (the "Ch0wn Domain").

9. Law enforcement received subscriber information for the Ch0wn Domain from the domain name provider, which revealed "User ID" associated with the Ch0wn Domain was "anonops31337," and the user's email address was "anonops31337@gmail.com" (the "Anonops Gmail Account"). According to the subscriber records, the Ch0wn Domain was paid for by a person identified as "LAURI LOVE" who used the email address "lauri.love@gmail.com" as the email address for the PayPal transaction (the "Lauri Love Gmail Account").

10. These same subscriber records also identified the IP address from which the PayPal payment for the Ch0wn Domain was made ("Ch0wn Payment IP Address"). Through open source investigation, law enforcement determined that the Ch0wn Payment IP Address was provided by an Internet Service Provider located in the United Kingdom (the "UK ISP"). Subscriber records obtained from the UK ISP identified the subscriber to the Ch0wn Payment IP Address as "Rev A.B. Love" with an address in Stradishall, England. Through financial inquiries and other investigative measures, law enforcement has determined that this location is the home address of defendant LAURI LOVE's parents.

11. Law enforcement obtained subscriber records from Google for the Lauri Love Gmail Account and the Anonops Gmail Account, which further confirmed that both of these accounts were connected to defendant LOVE.

a. First, the nickname identified in the subscriber records for the Lauri Love Gmail Account was "NSH." As described below, "NSH" is the name that defendant LOVE used to discuss and plan computer hacking in the IRC chats with the Co-Conspirators.

b. Second, the subscriber records for the Anonops Gmail Account identified the subscriber as "Smedley Butler," a known online pseudonym for defendant LOVE.

c. Third, NSH (i.e., defendant LOVE) referenced the Anonops Gmail Account in an online chat with another individual on or about October 4, 2012:

<Alias 4>: nsh
<Alias 4>: do you have an email address laying around that is not tied to a particular name?
<Alias 4>: as in, real name
<nsh>: to receive mail personally?
...
<nsh>: anonops31337 is associated with a made up person, but is tied to paypal usage[1]

12. Accordingly, the digital evidence relating to the October 2, 2012 attack on the Engineer R&D Center leads directly back to defendant LOVE.

C. The Identification of NSH as Lauri Love

13. Through open source investigation, law enforcement discovered an article in the September 8, 2012 issue of "The Observer" magazine entitled "Anonymous: behind the masks of the cyber insurgents," in which an Anonymous-affiliated individual with the moniker "NSH" was interviewed.[2] The reporter explained that she believed NSH was a college-aged British male at a prestigious university in the United Kingdom, which coincides with the observed British IP addresses attributed to him in this investigation.

14. Another open source search for the Lauri Love Gmail Account and NSH produced IRC chats between approximately 2005 and approximately 2011 in which an individual with the username of "NSH" and "n5h" gave his email address as lauri.love@gmail.com (i.e., the Lauri Love Gmail Account) and stated that Lauri Love was his legal name. The search also disclosed the existence of a Twitter account, @laurilove (named "Smedley Butler"), which had last been used on or about October 25, 2011. The account owner used the hashtag "#nshmarks" and listed his email as lauri.love@gmail.com.

---

[1] The text of the chats is reproduced in the Complaint as it appears in the chat logs I have reviewed; errors in spelling and punctuation have not been corrected. Each participant in a chat is identified by an alias. For example, <nsh> indicates a statement from LAURI LOVE using the alias "nsh." Where statements from individuals other than the defendant are reproduced herein, those individuals' aliases have been redacted and replaced with "Alias 1," "Alias 2," etc., as appropriate. Based upon my training and experience, my participation in the investigation, and my familiarity with language used on the Internet, I have included certain interpretations of the overall content of selected chats.

[2] Available at http://www.guardian.co.uk/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents?INTCMP=SRCH.

D. The Other Military Attacks

15. The investigation has revealed that several additional USM computer servers were attacked between in or around October 2012 and in or around January 2013 using the methods described above.

The Army Network Enterprise Technology Command ("NETCOM") Attack

16. Beginning on or about October 6, 2012, and continuing through on or about October 9, 2012, NETCOM was the victim of a SQL Injection Attack. The Co-Conspirators unlawfully accessed data from NETCOM servers which included personally identifiable information of over 1,000 individuals, including active military personnel.

17. On or about October 6, 2012, the Co-Conspirators discussed this hack in an IRC chat, including some of the data that they had accessed from the NETCOM servers:

<nsh>	[Alias 5]
<nsh>	you hexing mil?
< Alias 5>	Yes
< Alias 5>	sure am!
< Alias 5>	Via my new vps
< Alias 5>	lol
< Alias 5>	hmm, have a look at some of the passwords, hmm
<nsh>	okais

Based on my training and experience, and the context of this conversation, I am aware that the term "hexing" is another word for hacking, and therefore I believe that the phrase "hexing mil," is a reference to hacking military computer servers. Also, based on my training and experience, and the context of the conversation, I believe that the phrase "[v]ia my new vps," is a reference to hacking conducted through a virtual private server. Virtual private servers, which can be used to mask the identity of the user of a particular IP address, are often used by computer hackers.

18. Also on or about October 6, 2012, defendant Love stated in an IRC chat simply "hacking the army."

The Army Contracting Command Attack

19. Beginning on or about October 7, 2012, and continuing through on or about October 8, 2012, the Army Contracting Command's Army Materiel Command located in or around Redstone Arsenal, Alabama was the victim of a SQL Injection Attack through which the Co-Conspirators unlawfully accessed nonpublic data from an ACC database, including competitive acquisition bids and related attachments.

20. On or about October 10, 2012, in an IRC chat, defendant Love indicated that he had hacked the ACC website.

The Army Corps Attack

21. Beginning on or about October 7, 2012 and continuing through October 9, 2012, the Army Corps in Vicksburg, Missouri was the victim of a SQL Injection Attack that unlawfully exposed nonpublic data from an Army Corps database, including engineering best practices documents and other engineering documents.

22. The Co-Conspirators, including defendant Love, discussed this hack in an IRC chat on or about October 7, 2012. Specifically, the Co-Conspirators discussed the data that they stole from the Army Corps database, including email addresses of military personnel:

< Alias 5> 400K email log?
...
<Alias 5> The other army one is almost completely dumped :)
<nsh> nicee
<Alias 5> Oh
<Alias 5> Wow
<Alias 5> We're going to have 400k emails.
...
<nsh> can you grab one email for curiosity
<nsh> to see who from to about

The Plans and Analysis Integration Office Attack

23. On or about October 9, 2012, the Co-Conspirators compromised a computer server owned and operated by PAIO's Research, Development and Engineering Command, located in or around Aberdeen Proving Ground, Maryland. The Co-Conspirators unlawfully accessed chemical and biological defense program budgeting data, among other information.

24. On or about the date of the hack, defendant LOVE and a Co-Conspirator discussed the attack in an IRC chat:

<nsh>: how did you get this shell?
<Alias 5>: got the shell from coldfusion vuln

Based on my training and experience, and the context of this conversation, I am aware that the term "shell" often is used by computer hackers to describe a "backdoor" or other means of accessing a computer server connected to the Internet. Accordingly, I believe that the above excerpt is a reference to exploiting the PAIO's computer servers using a vulnerability in the Coldfusion web application development platform.

The December 23, 2012 Engineer R&D Center Attack

25. On or about December 23, 2012, the Co-Conspirators again attacked a computer server located at the Engineer R&D Center. The intrusion continued through on or about January 2, 2013.

26. As with previous attacks, the Co-Conspirators exploited a vulnerability in the server's ColdFusion platform and unlawfully accessed several USM databases, which included information regarding natural resource management and construction engineering research, among other things.

27. In carrying out this attack, the Co-Conspirators used a compromised computer server located in Parsippany, New Jersey, to temporarily store malicious files that they then used to carry out the intrusion.

The Strategic Studies Institute Attack ("SSI")

28. On or about January 11, 2013, the Co-Conspirators compromised a server owned and operated by SSI by exploiting a vulnerability in the network's ColdFusion platform.

29. On or about January 11, 2013, defendant LOVE, using the online moniker "peace," discussed this hack in an IRC chat. Among other things, defendant LOVE posted a link to the "shell" that the Co-Conspirators had used, and could continue to use, in order to access SSI's server.

E. Other Hacks

30. In addition to the above-described military hacks, law-enforcement has reviewed IRC chats in which the Co-Conspirators discussed, planned, and took credit for numerous other cyber attacks against military and governmental agencies between in or about October 2012 and in or about February 2013, including the United States Sentencing Commission and the Federal Reserve.